International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 2

(09/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.800-X.849 series – Supplement on security baseline for network operators

ITU-T X-series Recommendations – Supplement 2

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

For further details, please refer to the list of ITU-T Recommendations.

Supplement 2 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on security baseline for network operators

Summary

Supplement 2 to ITU-T X.800 series of Recommendations defines a security baseline against which network operators can assess their network and information security status in terms of readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats. This supplement can be used by network operators to provide meaningful criteria against which each network operator can be assessed if required.

Source

Supplement 2 to ITU-T X-series Recommendations was agreed on 28 September 2007 by ITU-T Study Group 17 (2005-2008).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Supplement 2 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on security baseline for network operators

1 Scope

Nowadays, there are thousands of network operators, ranging from long-established national incumbents (who have trusted each other for many years) to small, start-up networks with no track record and no real basis of establishing trust, so new problems that did not exist in the traditional regulated environment are now emerging. It is necessary for operators to know who they are dealing with and the extent to which they can trust other operators to avoid the security problems. Security baseline is the response to this new challenge.

The use of this supplement might vary from country to country, according to regulatory regimes. Some regulatory regimes may choose to require that network operators follow the requirements of this supplement. Some network operators may themselves require that other network operators meet certain level of security as a prerequisite to the interconnection.

It is recommended that an operator provide telecommunication service for users at the security level that is guaranteed by the implementation of this supplement. The services of higher security level may be provided on customer's demand by the operator at a cost to the former.

This supplement is organized into three groups: operator's policy baseline and implementation, technical tools baseline and collaboration baseline. These must be capable of being verified. Evaluation might be conducted by an operator itself as a declaration procedure or with the assistance of the evaluation body through the compliance certification.

NOTE – This security baseline includes both technical and management-oriented tools.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 risk management: Coordinated activities to direct and control an organization with regard to risk [b-ISO/IEC 27001].

3.1.2 security policy: The set of rules laid down by the security authority governing the use and provision of security services and facilities [b-ITU-T X.509].

3.1.3 unauthorized access: An entity attempts to access data in violation of the security policy in force [b-ITU-T M.3016].

3.2 Terms defined in this supplement

This supplement defines the following terms:

3.2.1 antiviral software: Computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (maleware).

3.2.2 distributed denial of service (DDoS): In the context of message handling, when an entity fails to perform its function or prevents other entities from performing their functions, which may be a denial of access, a denial of communications, a deliberate suppression of messages to a particular recipient, traffic flooding, an MTA was caused to fail or operate incorrectly, an MTS was caused to deny a service to other users. DDoS threats include denial of communications, MTA failure, MTS flooding.

3.2.3 license agreement: Agreement between owner of the software and the user of its copy.

3.2.4 network operator: An organization which operates a telecommunications network.

3.2.5 network operator's information security: The state of the network operator's information resources and infrastructure protection from random and deliberate influence, natural or artificial, that can cause damage to the network operator and users of communication services. It is characterized by the ability to maintain confidentiality, integrity and accessibility of information during it storage, processing and transmission.

3.2.6 point of interconnect: The point where the operator connects users (or other operators) to the data transmission service with the declared quality.

3.2.7 service provider: An entity that offers services to users involving the use of network resources.

3.2.8 spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk of messages. (Spam affects e-mail, short message systems, IP multimedia systems and other communication systems.)

4 Abbreviations and acronyms

This supplement uses the following abbreviations:

DDoS Distributed Denial of Service

IDS Intrusion Detection Service

IPS Intrusion Prevention Service

IRT Incident Response Team

MTA Message Transfer Agent

MTS Message Transfer System

5 Conventions

None.

6 Operator's policy baseline and implementation

6.1 Network operators' information security provisions must comply with regulatory and legal requirements of the jurisdiction in which the operator is engaged in business activity. In addition, network operators must meet local jurisdiction requirements regarding cooperation with law enforcement agencies.

6.2 It is recommended that the operator adopt a security policy that is based on recognized best practices (such as [b-ISO/IEC 27002] and [b-ITU-T X.1051]) and risk assessment, that meets the demands of business activity, that complies with national legislation and that is in accordance with the internal network operator procedures. It is recommended that operators' personnel and external participants (users, interconnected operators and other interested parties) be made aware of the requirements of the security policy.

6.3 It is recommended that the operator's security policy have a clause dedicated to delimitation of responsibility within the operator's personnel, between the operator and its partners, and between the operator and its customers.

6.4 It is recommended that the information security requirements that must be followed by personnel be included in the labour contracts (job specification, list of duties) of all employees dealing with publicly-accessible information resources.

6.5 Measures implemented to protect an operator's resources or the resources of its customers, should not result in harmful consequences for third parties in an information exchange, nor should any side effects of their deployment cause damage or inconvenience that exceeds the impact of the risk being mitigated.

6.6 It is recommended that network operators work collaboratively to address risks and vulnerabilities.

6.7 Implementation of security facilities should address the reduction of risk and the cost of such measures should reflect the value of the assets protected and the potential damage.

7 Technical tools baseline

7.1 It is recommended that the operator deploy all hardware and software in strict correspondence with the terms of license agreement, defined by the manufacturer.

7.2 It is recommended to only use individual accounts for access to the interfaces of communication hardware management. The deployment of group accounts is not recommended.

7.3 It is recommended that default passwords (set by the manufacturer of the hardware or software) not be used to authorize access to network management interfaces, remote consoles or management and administrative accounts of any communication hardware and/or software.

7.4 It is recommended that the operator install updates and patches in a timely manner as recommended by the manufacturer. It is recommended that the operator bring to the notice of users of the facilities, information about applicable patches and updates.

7.5 It is recommended that the information relating to the network management system be protected by confidentiality and integrity mechanisms or by using network segments physically isolated from service domains.

7.6 It is recommended to install anti-spoofing filters at the points of interconnect with other networks (operators) and end-users, which prevent the transmission of packages with the outgoing addresses from external networks or multicast addresses, as well as receiving packages with such addresses or with reserved or incorrect addresses.

7.7 It is recommended that inspected packages be labelled so that interconnected operators know that the outgoing address is correct. In case of traffic congestion, the labelled packages should be prioritized.

7.8 It is recommended that network operators and public information server owners deploy regularly-updated anti-viral software.

7.9 It is recommended to have facilities for detecting infected messages, marking and optionally deleting them.

7.10 It is recommended that each e-mail information server be enabled with spam-detecting software for all incoming messages and the possibility to mark messages with unsolicited information. The operators may use other methods for counteracting spam. For instance, they could, by prior agreement, disconnect users connected to the networks manipulated by violators.

7.11 It is recommended that operators filter spam within their own network.

7.12 It is recommended that each e-mail server have the ability to limit the amount of outgoing messages from one user within a unit of time (e.g., for protecting against spam or denial of service attacks). It is recommended to have the ability to delay the delivery of outgoing messages by such sender until the server administrator confirmation is obtained.

7.13 It is recommended that the operator deploy automated discovery of statistical traffic anomalies. It is recommended that such traffic anomaly analysis be used for effective counteraction to DDoS attacks.

7.14 It is recommended that the operator deploy technical and organizational measures that allow it to determine the source of a violation (e.g., a DoS attacks) and to block (de-activate) the attacks.

7.15 It is recommended that regularly-updated intrusion detection and prevention services (IDS/IPS) be applied to handle selective real-time contextual traffic analysis for the traffic received from users and other operators.

7.16 It is recommended that operators assure the confidentiality of transmitted and/or stored information related to management and billing systems, personal user data and information about services provided to users.

7.17 It is recommended that logs of detected incidents be stored for a sufficient period of time to facilitate the investigation of incidents. It is recommended that technical correlation tools be deployed to assess information from all available security logs.

7.18 It is recommended that operators offer the capability to selectively block or filter traffic by means of regular network equipment features, at the request of the user.

7.19 It is recommended that routine control facilities be used for configuration and maintenance of the security settings of communication facilities and management network elements (including firewalls, routers and servers). Personnel activities on the communication facility should be logged.

7.20 It is recommended that the operator use approved best security practices (such as [b-ISO/IEC 27002] and [b-ITU-T X.1051]) whenever developing applications and services for end-users (for example, when offering self-service capabilities to the users).

7.21 Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This should be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g., avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.

8 Collaboration baseline

8.1 It is recommended that the operator help customers (end-users) and service providers recognize risks that arise from the use of network services. The operator should inform users about fundamental risks that arise from the network and about counter-measures against these risks aimed at the reduction of damage.

8.2 It is recommended to have the facilities to identify all users, partners and other operators that are involved in the direct interaction on the network.

8.3 It is recommended that operators have the ability to determine the jurisdiction (i.e., the territory or state) in which a publicly-available information network resource is located.

8.4 It is recommended that operators have the ability to obtain information about the owner (administrator) of a publicly-available information network resource for purposes of incident investigation or resolution.

8.5 It is recommended that the operator promptly inform all affected parties in the event of leakage of a user's data, or the data of an interconnected operator.

8.6 The operator should recommend to its enterprise users (legal entities) that they appoint personnel responsible for the information security of corporate resources. Such employees should have sufficient qualifications and authority to counteract security threats.

8.7 It is recommended that the operator inform users about widespread threats relating to the use of services and information resources or provide users with a link to trustworthy information thereof, and educate the users about settings in the edge network equipment allowing to ensure information security.

8.8 It is recommended that the operator have a round-the-clock incident response team (IRT) or use an outsourced IRT.

8.9 It is recommended that the operator's IRT be accessible via the phone and e-mail for authorized customers' or interconnected operators' representatives in accordance with the operator's policy and/or communication service agreement. Incidents should be investigated based on recognized best practices.

8.10 It is recommended that the operator stipulate, in its service level agreement, a clause on procedures for informing its users, within a short period of time, about discovered vulnerabilities in hardware or software that can cause negative consequences to them, mainly those respecting their privacy. The notification of vulnerabilities should also be sent by the operator to concerned equipment manufacturers. The agreement should contain a comprehensive statement of security requirements, which, should they be violated, will cause suspension or termination of communication services to the customer.

Bibliography

[b-ITU-T M.3016] ITU-T Recommendation M.3016.x series (2005), *Security for the management plane*.

[b-ITU-T X.509] ITU-T Recommendation X.509 (2005), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1051] ITU-T Recommendation X.1051 (2004), *Information security management system – Requirements for telecommunications (ISMS-T)*.

[b-ISO/IEC 17799] ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008